IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

US MedRehab, LLC,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No.
	)	
JOHN DOE,	)	
	)	
Defendant.	)	

COMPLAINT

Plaintiff US MedRehab, LLC ("USMR"), through its undersigned counsel, hereby files this Complaint requesting damages, and alleges as follows:

INTRODUCTION

1. USMR files this action to assert a claim for violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CAFAA") in connection with "click fraud" perpetrated by an unidentified "John Doe" Defendant. USMR has arrangements with online advertisers whereby it pays a fee for each click received by links that advertiser makes available to the public (i.e, "pay-per-click"), which directs the public to USMR's website where they can learn about and potentially purchase USMR's products.

2. Beginning in early 2022, unknown Defendant John Doe has engaged in a campaign of repeatedly clicking USMR's online advertisements without any interest in or intention of purchasing USMR's products for the purpose of increasing the fees USMR must pay to its advertising partner, and/or causing USMR's advertisements not to appear once its advertising budget is depleted.

3. Plaintiff seeks damages for the inflated advertising costs incurred by this fraudulent activity, loss of potential customers, and the corruption of its data caused by the insertion of these fraudulent clicks.

THE PARTIES

4. Plaintiff US MedRehab, LLC, is a Missouri Limited Liability Company with its headquarters in St. Louis, Missouri. Plaintiff is in the business of selling medical rehabilitation equipment online through its website (www.usmedrehab.com) and its telephone sales line. USMR relies on sales from its website for the bulk of its business.

5. USMR has contracts with third-party online advertisers who direct traffic to referral links, intended to connect people who have a need for medical rehabilitation equipment with USMR's website. USMR then pays those third-party online advertisers based on the number of clicks it receives to the referral link from the general public. USMR relies on those clicks being from *bona fide* potential customers genuinely interested in the products it sells.

6. Defendant John Doe is an individual who has clicked or caused to be clicked the referral links USMR has published through third-party advertisers thousands of times, apparently using automated programs such as malware or automated bots.

7. USMR cannot ascertain John Doe's actual identity without information from his or her Internet Service Provider ("ISP").

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over USMR's CAFAA claim under 18 U.S.C. § 1030 (CAFAA) and 28 U.S.C. § 1331 (actions arising under the laws of the United States).

9. This Court has personal jurisdiction over John Doe under the Missouri long-arm statute, Mo. Rev. Stat. § 506.500.1, which authorizes jurisdiction within Missouri for claims arising out of "the commission of tortious acts within the state[.]" *Id.* That phrase includes "extraterritorial acts producing actionable consequences in Missouri." *Fulton v. Chicago, Rock Island & P. R. Co.*, 481 F.2d 326, 331 (8th Cir. 1973) (collecting cases). Here, even if the overt actions John Doe performed to undertake the click fraud occurred outside of Missouri, the actionable consequences are nevertheless felt by USMR inside of Missouri.

10. Venue is proper in this district pursuant to 28 U.S.C. § 1391(b), because a substantial part of the events giving rise to the claims in this action occurred in this District.

FACTUAL ALLEGATIONS

11. USMR sells equipment used for medical rehabilitation using its website and telephone sales line. USMR's warehouse is located in Missouri, but it advertises, receives orders from, and ships to locations across the country.

12. USMR spends significant resources directing advertisements to potential customers, most of which is in the form of online advertisements. USMR uses advertising services provided by third-parties, including Microsoft's "Bing" search engine, to create and display its online advertisements.

13. Microsoft uses a payment model that charges USMR for each click to its advertisements. USMR and Microsoft set a budget cycle cap, such that the advertisement will not appear once the budget is depleted until the next budget cycle.

14. Microsoft's pay-per-click model creates the potential for "click fraud" whereby an individual or business can target a company and direct clicks to the posted advertisement that are not connected with any desire to purchase the product. The result of these efforts is to increase

the advertising spending without bringing any new customers, and potentially to accelerate the removal of the advertisement by causing the target to hit the budget cycle advertising cap when it otherwise would not. The potential motives for click fraud are numerous, as it may be perpetrated by a target's competitors, disgruntled customers, former employees, or simply anonymous vandals.

15. Click fraud can be performed manually by clicking the advertisement multiple times at a computer, or else it can also be performed via automated processes such as malware or bots that are capable of sending many times the number of clicks that a human could perform.

16. Starting in January of 2022, USMR's click fraud detection software found that it was receiving multiple repeated clicks to its advertisements from an unidentified John Doe. On information and belief, these clicks are not the result of John Doe's interest in purchasing products from USMR but rather appear directed to artificially and maliciously inflating USMR's expenses associated with advertising on a pay-per-click basis. USMR's software indicated that the clicks were likely the result of malware or bots clicking the link repeatedly in an automated fashion.

17. USMR has tracked John Doe to his Internet Protocol Address ("IP Address") on more than one occasion. Below is a list of the dates and IP Addresses USMR has been able to associate with John Doe's automated clicks to the referral links:

a. On January 26, 2022, at IP Addresses: 167.172.244.164,[1] 167.172.248.39,[2] 128.199.12.1,[3] and 137.184.83.19;[4]

b. On January 27, 2022, at IP Address: 143.244.165.196;[5]

[1] On information and belief, this IP address is associated with a location in Clifton, New Jersey.
[2] On information and belief, this IP address is associated with a location in Clifton, New Jersey.
[3] On information and belief, this IP address is associated with a location in Santa Clara, California.
[4] On information and belief, this IP address is associated with a location in Santa Clara, California.

c. On February 7, 2022, at IP Addresses: 164.90.137.183,[6] 159.65.237.85,[7] and 143.198.78.35;[8]

d. On February 3, 2022, at IP Addresses: 161.35.238.31,[9] 157.245.248.141,[10] 137.184.210.244,[11] 134.122.112.123,[12] 137.184.145.113,[13] 143.198.98.255,[14] 137.184.145.113,[15] 159.223.171.130,[16] 143.198.78.35,[17] 164.90.157.79,[18] 137.184.67.229;[19] and

e. On February 11, 2022, at IP Address: 68.183.120.5. [20]

18. USMR believes that the traffic originated from a single user, because the associated IP Addresses correspond to approximately the same three geographic locations, sometimes on the same day.

19. In an effort to identify John Doe, USMR reached out to the company it was able to determine was John Doe's ISP to learn whether any steps could be taken to stop this conduct or to provide information necessary to identify John Doe. True and accurate copies of correspondence to the ISP associated with these IP Addresses are attached hereto as Exhibits 1, 2, 3, 4, and 5.

---

[5] On information and belief, this IP address is associated with a location in North Bergen, New Jersey.
[6] On information and belief, this IP address is associated with a location in Clifton, New Jersey.
[7] On information and belief, this IP address is associated with a location in North Bergen, New Jersey.
[8] On information and belief, this IP address is associated with a location in Santa Clara, California.
[9] On information and belief, this IP address is associated with a location in Santa Clara, California.
[10] On information and belief, this IP address is associated with a location in North Bergen, New Jersey.
[11] On information and belief, this IP address is associated with a location in North Bergen, New Jersey.
[12] On information and belief, this IP address is associated with a location in North Bergen, New Jersey.
[13] On information and belief, this IP address is associated with a location in North Bergen, New Jersey.
[14] On information and belief, this IP address is associated with a location in Santa Clara, California.
[15] On information and belief, this IP address is associated with a location in North Bergen, New Jersey.
[16] On information and belief, this IP address is associated with a location in North Bergen, New Jersey.
[17] On information and belief, this IP address is associated with a location in Santa Clara, California.
[18] On information and belief, this IP address is associated with a location in Santa Clara, California.
[19] On information and belief, this IP address is associated with a location in North Bergen, New Jersey.
[20] On information and belief, this IP address is associated with a location in North Bergen, New Jersey.

20. Despite assurances from John Doe's ISP that it had taken steps to prevent further attacks, the click fraud persisted. John Doe's ISP refused to divulge any identifying information regarding John Doe in response to informal requests.

21. USMR has been substantially harmed by John Doe's anonymous click fraud, and it will continue to be harmed if this activity continues.

22. Despite USMR's efforts, it has been unable to identify John Doe responsible for these attacks.

COUNT I – VIOLATION OF 18 U.S.C. § 1030 (CAFAA)

23. USMR repeats and incorporates as if set forth fully herein the allegations contained in the foregoing paragraphs.

24. Microsoft's computers are used in and affect interstate commerce and communication, and thus are protected computers.

25. USMR's computers are used in and affect interstate commerce and communication, and thus are protected computers.

26. Intending to defraud USMR and potentially reap a benefit, John Doe caused USMR's online advertisements to be clicked repeatedly. Those advertisements are stored on Microsoft's computers.

27. On information and belief, John Doe did not cause USMR's advertisements to be clicked due to a genuine interest in learning about or purchasing medical rehabilitation equipment. Rather, on information and belief, John Doe intends to attack USMR, either in an effort to impose additional pay-per-click costs on USMR, reduce its advertising budget, and accelerate the pace by which USMR's advertisements are removed from Microsoft's Bing search

results. On information and belief, John Doe does this to obtain a competitive or other monetary advantage.

28. By clicking USMR's online advertisements, John Doe accessed Microsoft's protected computers, because each click sent an electronic instruction to Microsoft's computers, which interpreted it as interest in USMR's advertisement, which in turn redirected John Doe to USMR's website.

29. By clicking USMR's online advertisements and being redirected to USMR's website, John Doe also transmitted fraudulent data to USMR's computer system. A click of USMR's advertising link ultimately sends a request to USMR's system to display its website. USMR uses data it obtains from *bona fide* clicks redirecting to its website to determine facts such as the volume, location, and frequency of customer interest, for the purposes of tailoring its advertisement strategy, including its budget. USMR's use of this request data requires that the incoming referrals are from people who are genuinely interested in learning about or purchasing medical rehabilitation equipment. John Doe therefore caused this data to be corrupted by inserting its own fraudulent clicks, which do not reflect the genuine interest of a potential customer.

30. By clicking USMR's advertisements without any interest in its website or equipment, John Doe exceeded his or her authorized access to Microsoft's protected computers, furthered their fraud, and obtained things of value in violation of 18 U.S.C. § 1030(a)(4).

31. By clicking USMR's advertisements without any interest in its website or equipment, John Doe knowingly caused the transmission of information that intentionally caused damage to USMR's data stored on its protected computers in violation of 18 U.S.C. § 1030(a)(5)(A).

32. As a result of John Doe's unauthorized access, USMR has incurred losses of more than $5,000 in the span of less one year, in the form of additional pay-per-click costs and lost sales.

33. On information and belief, as a result of John Doe's unauthorized access, potential customers of USMR may have suffered potential modification or impairment of medical treatment or care by reduced access to medical rehabilitation equipment.

PRAYER FOR RELIEF

WHEREFORE, USMR prays for judgment against John Doe as follows:

1. For an award of compensatory damages to be proven at trial arising from John Doe's violations of 18 U.S.C. § 1030;

2. For such other and additional relief as the Court deems just and proper.

Respectfully submitted,

CARMODY MACDONALD P.C.

By: /s/ Christopher J. Lawhorn

Christopher J. Lawhorn, # 45713MO
120 South Central Avenue, Suite 1800
St. Louis, Missouri 63105
(314) 854-8600 Telephone
(314) 854-8660 Facsimile
cjl@carmodymacdonald.com

Attorneys for Plaintiff US MedRehab, LLC